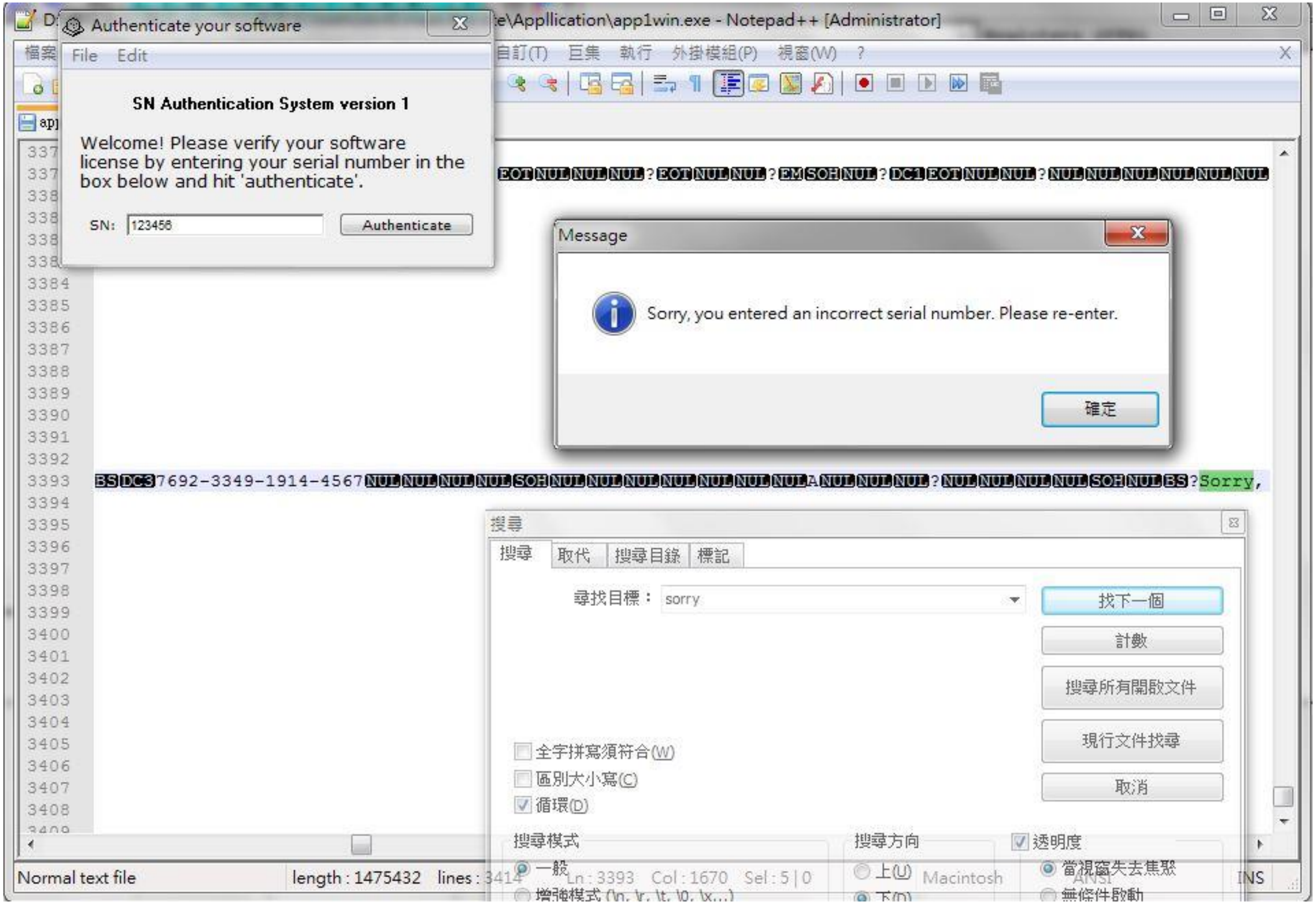
INFORMATION SECURITY

LABORATORY

2016/05/24

HTS Application 1

- Just Notepad++ .



Authenticate your software

SN Authentication System version 1

Welcome! Please verify your software license by entering your serial number in the box below and hit 'authenticate'.

SN: 123456

Message

Sorry, you entered an incorrect serial number. Please re-enter.

```
EOTNULNULNUL?EOTNULNUL?EMSOHNUL?DC1EOTNULNUL?NULNULNULNULNULNUL
BSDC37692-3349-1914-4567NULNULNULNULSOHNULNULNULNULNULNULNULANULNULNUL?NULNULNULNULSOHNULBS?Sorry,
```

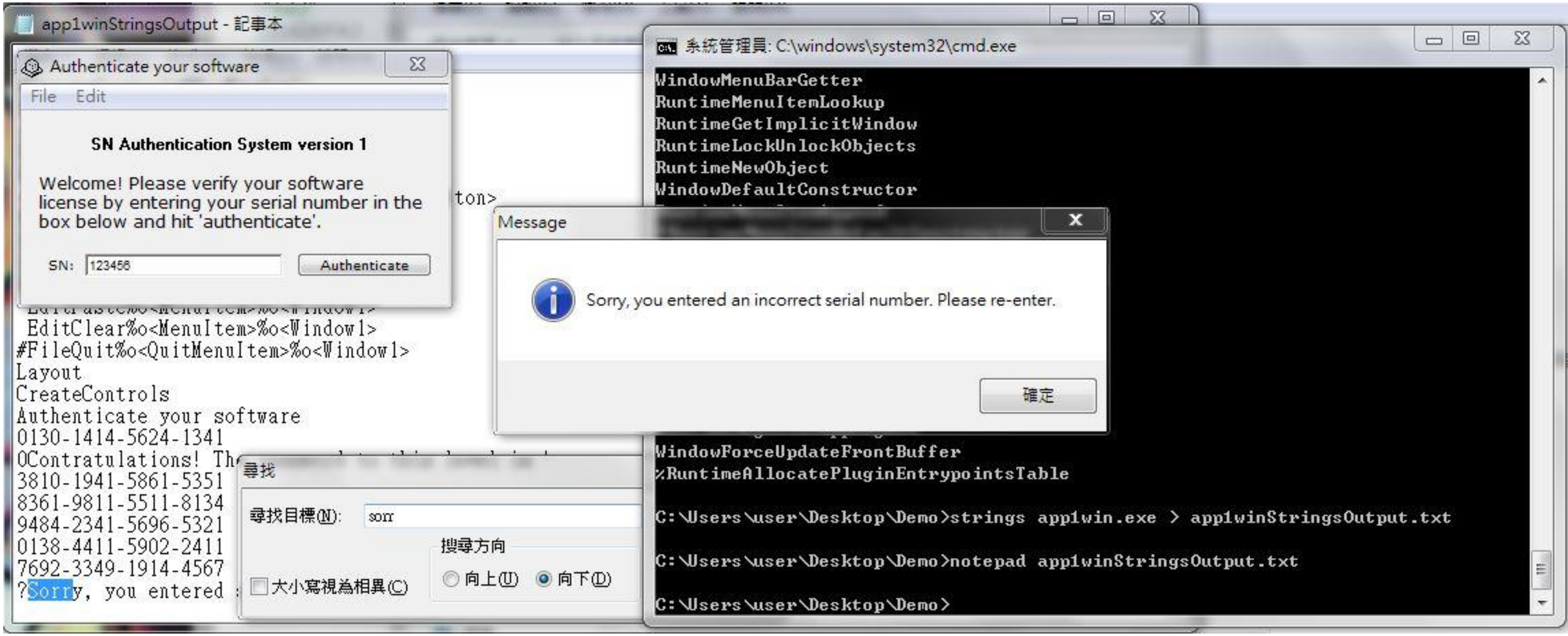
尋找目標： sorry

☐ 全字拼寫須符合(W)
☐ 區別大小寫(C)
☑ 循環(D)

Normal text file length : 1475432 lines : 3414 Ln : 3393 Col : 1670 Sel : 5 | 0

HTS Application 1

- Use tool to take all strings.



app1winStringsOutput - 記事本
Authenticate your software
File
Edit
Authenticate
Message
確定
尋找
搜尋方向
□大小寫視為相異(C)
○向上(U)
●向下(D)
系統管理員: C:\windows\system32\cmd.exe

SN Authentication System version 1

Welcome! Please verify your software license by entering your serial number in the box below and hit 'authenticate'.

SN: 123456

Sorry, you entered an incorrect serial number. Please re-enter.

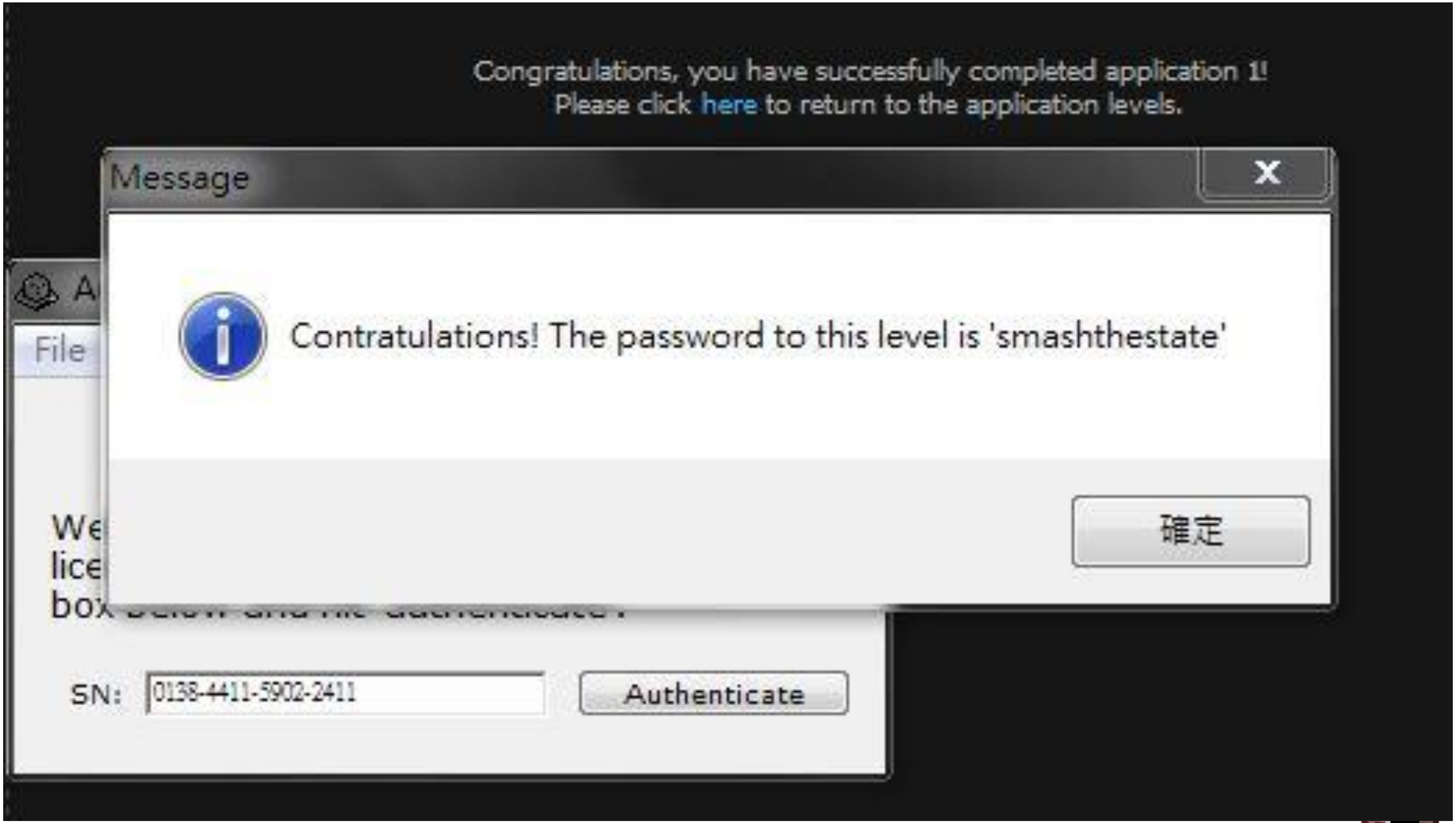
尋找目標(N): sorr

```
ton>
 EditClear%o<MenuItem>%o<Window1>
#FileQuit%o<QuitMenuItem>%o<Window1>
Layout
CreateControls
Authenticate your software
0130-1414-5624-1341
0Contratulations! Th
3810-1941-5861-5351
8361-9811-5511-8134
9484-2341-5696-5321
0138-4411-5902-2411
7692-3349-1914-4567
?Sorry, you entered :
```

```
WindowMenuBarGetter
RuntimeMenuItemLookup
RuntimeGetImplicitWindow
RuntimeLockUnlockObjects
RuntimeNewObject
WindowDefaultConstructor
WindowForceUpdateFrontBuffer
%RuntimeAllocatePluginEntrypointsTable

C:\Users\user\Desktop\Demo>strings app1win.exe > app1winStringsOutput.txt

C:\Users\user\Desktop\Demo>notepad app1winStringsOutput.txt

C:\Users\user\Desktop\Demo>
```

HTS Application 1

- Password is "smashthestate"

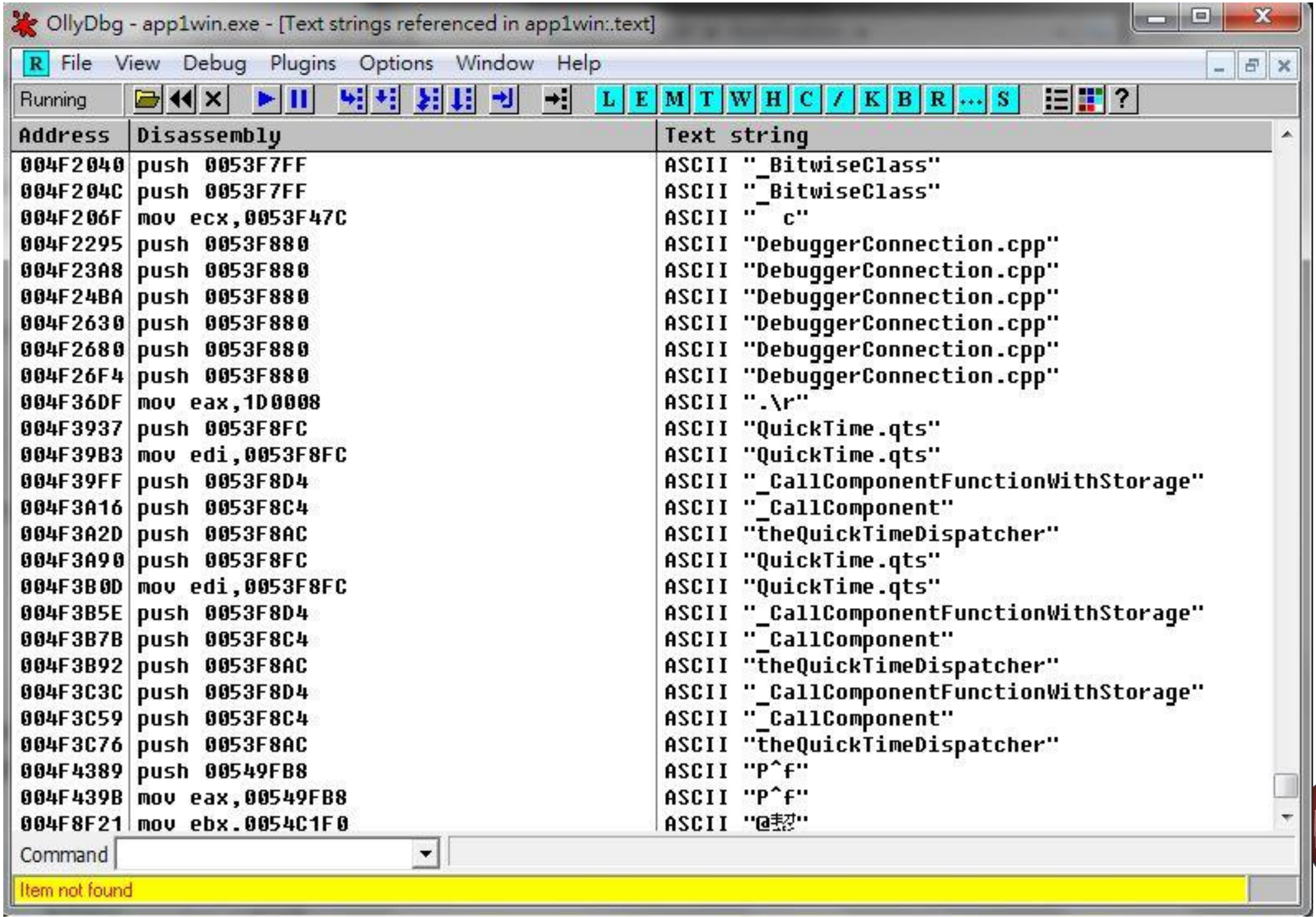


Congratulations, you have successfully completed application 1!
Please click here to return to the application levels.

Contratulations! The password to this level is 'smashthestate'

HTS Application 1

- Help!! What is those strings? (I can not find it in OllyDBG or IDApro. VB)



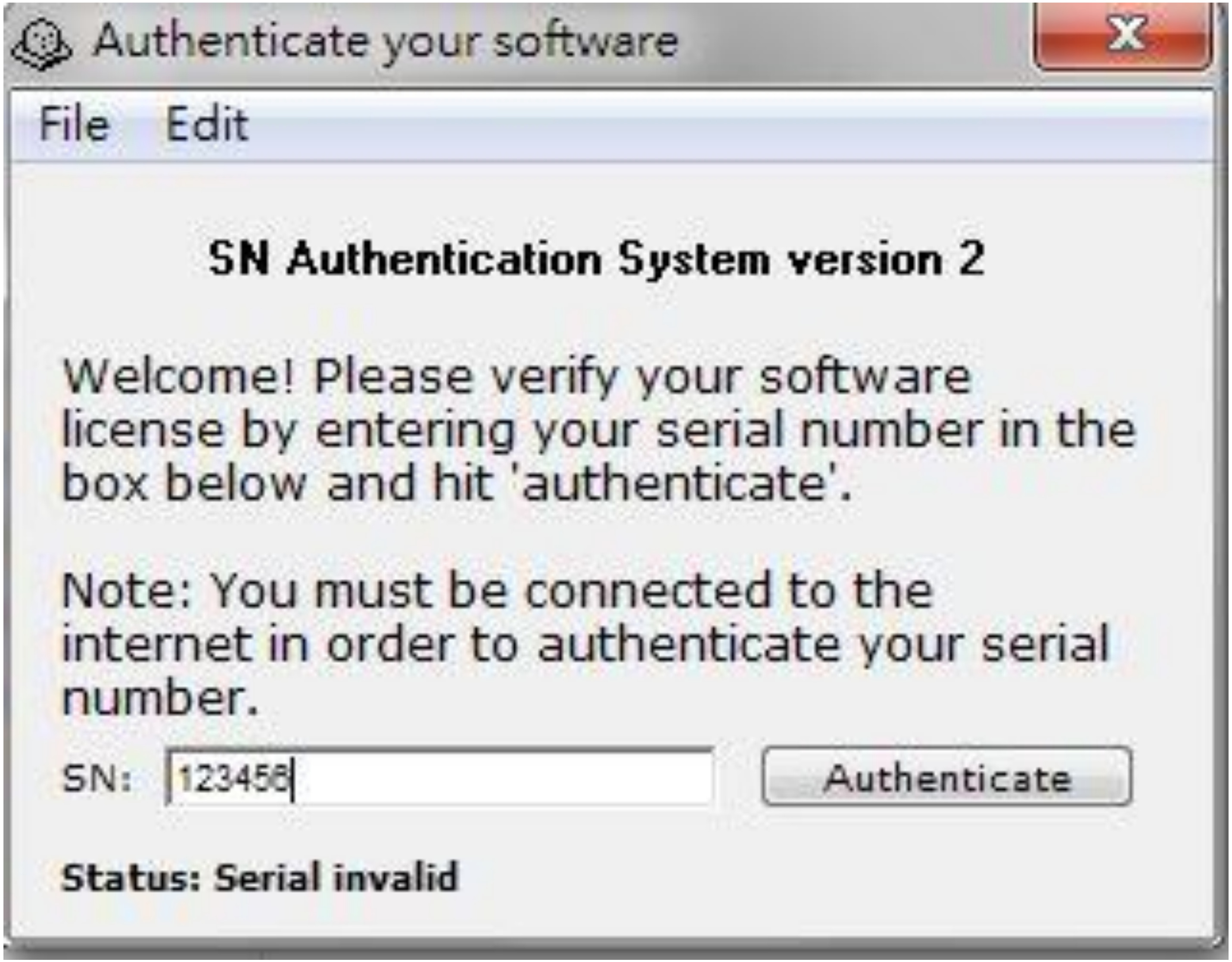
OllyDbg - app1win.exe - [Text strings referenced in app1win:.text]
R File View Debug Plugins Options Window Help
Running
L E M T W H C / K B R ... S ?
Command

```
Address   Disassembly          Text string
004F2040  push 0053F7FF        ASCII "_BitwiseClass"
004F204C  push 0053F7FF        ASCII "_BitwiseClass"
004F206F  mov ecx,0053F47C     ASCII "  c"
004F2295  push 0053F880        ASCII "DebuggerConnection.cpp"
004F23A8  push 0053F880        ASCII "DebuggerConnection.cpp"
004F24BA  push 0053F880        ASCII "DebuggerConnection.cpp"
004F2630  push 0053F880        ASCII "DebuggerConnection.cpp"
004F2680  push 0053F880        ASCII "DebuggerConnection.cpp"
004F26F4  push 0053F880        ASCII "DebuggerConnection.cpp"
004F36DF  mov eax,1D0008       ASCII ".\r"
004F3937  push 0053F8FC        ASCII "QuickTime.qts"
004F39B3  mov edi,0053F8FC     ASCII "QuickTime.qts"
004F39FF  push 0053F8D4        ASCII "_CallComponentFunctionWithStorage"
004F3A16  push 0053F8C4        ASCII "_CallComponent"
004F3A2D  push 0053F8AC        ASCII "theQuickTimeDispatcher"
004F3A90  push 0053F8FC        ASCII "QuickTime.qts"
004F3B0D  mov edi,0053F8FC     ASCII "QuickTime.qts"
004F3B5E  push 0053F8D4        ASCII "_CallComponentFunctionWithStorage"
004F3B7B  push 0053F8C4        ASCII "_CallComponent"
004F3B92  push 0053F8AC        ASCII "theQuickTimeDispatcher"
004F3C3C  push 0053F8D4        ASCII "_CallComponentFunctionWithStorage"
004F3C59  push 0053F8C4        ASCII "_CallComponent"
004F3C76  push 0053F8AC        ASCII "theQuickTimeDispatcher"
004F4389  push 00549FB8        ASCII "P^f"
004F439B  mov eax,00549FB8     ASCII "P^f"
004F8F21  mov ebx,0054C1F0     ASCII "@封"
```

Item not found

HTS Application 2

- Status will change.



SN Authentication System version 2

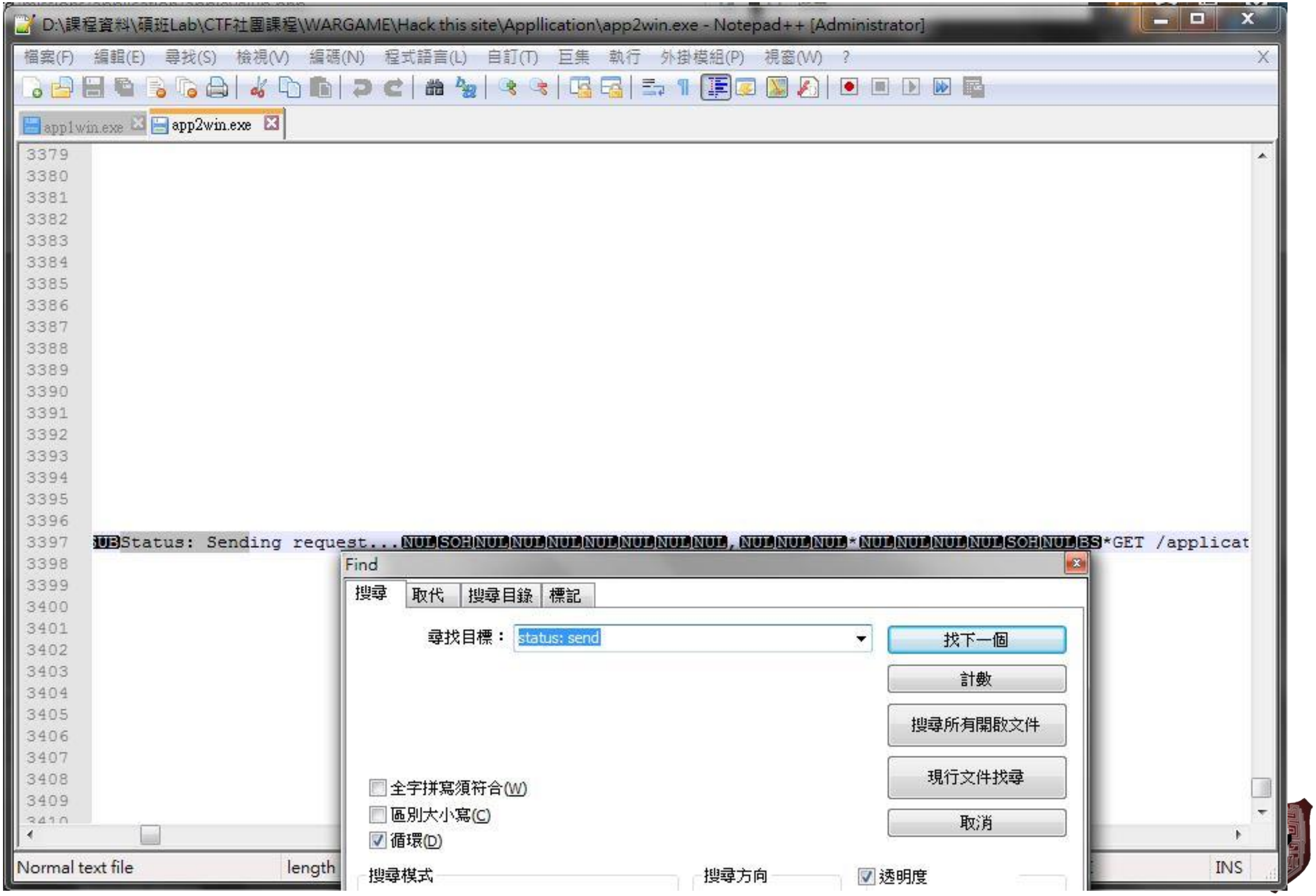
Welcome! Please verify your software license by entering your serial number in the box below and hit 'authenticate'.

Note: You must be connected to the internet in order to authenticate your serial number.

SN: 123456

Status: Serial invalid

HTS Application 2



D:\課程資料\碩班Lab\CTF社團課程\WARGAME\Hack this site\Appllication\app2win.exe - Notepad++ [Administrator]

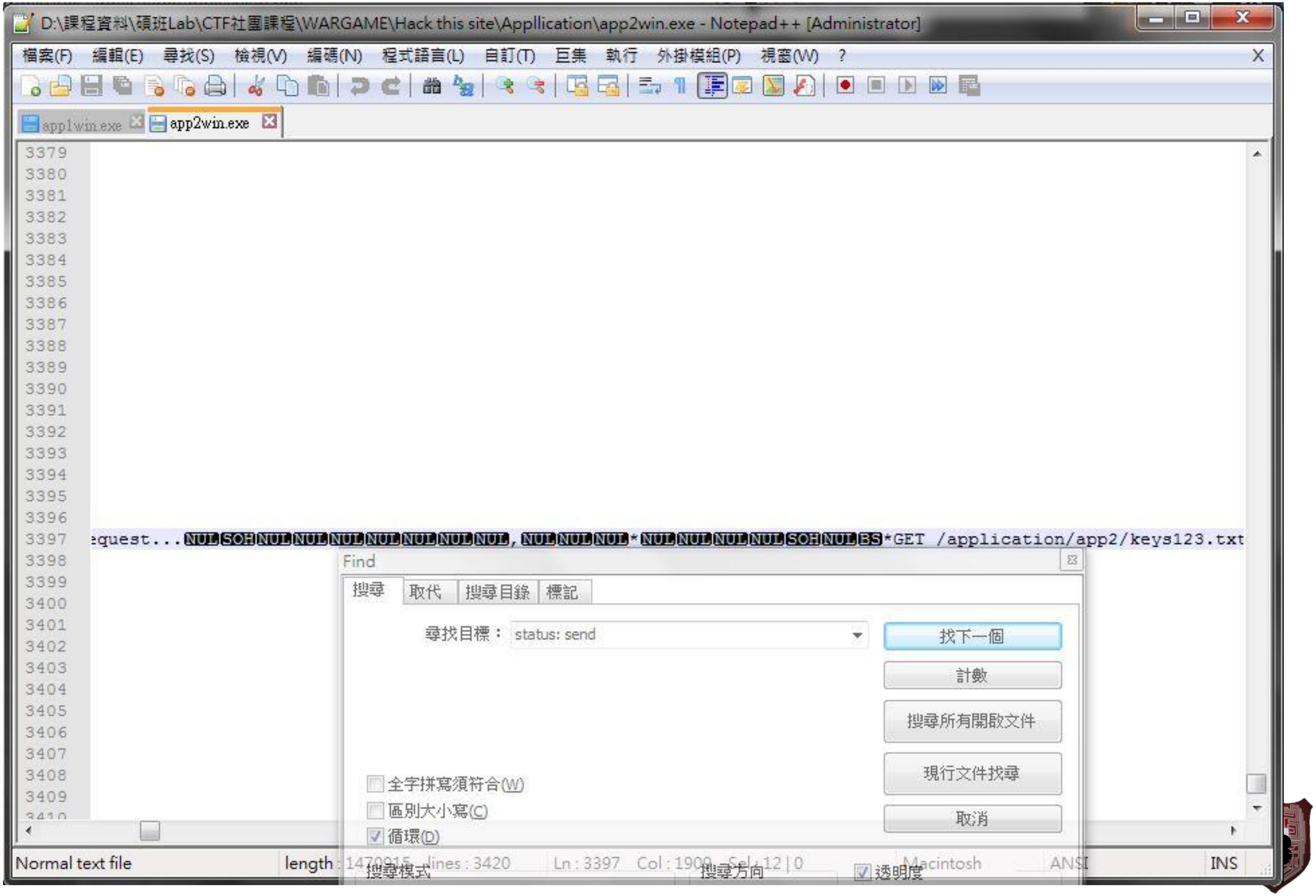
```
SUBStatus: Sending request...NULSOHNULNULNULNULNULNULNUL,NULNULNUL*NULNULNULNULSOHNULBS*GET /applicat
```

Find

尋找目標：status: send

☐ 全字拼寫須符合(W)
☐ 區別大小寫(C)
☑ 循環(D)
☑ 透明度

HTS Application 2



```
equest...NULSOHNULNULNULNULNULNULNUL,NULNULNUL*NULNULNULNULSOHNULBS*GET /application/app2/keys123.txt
```

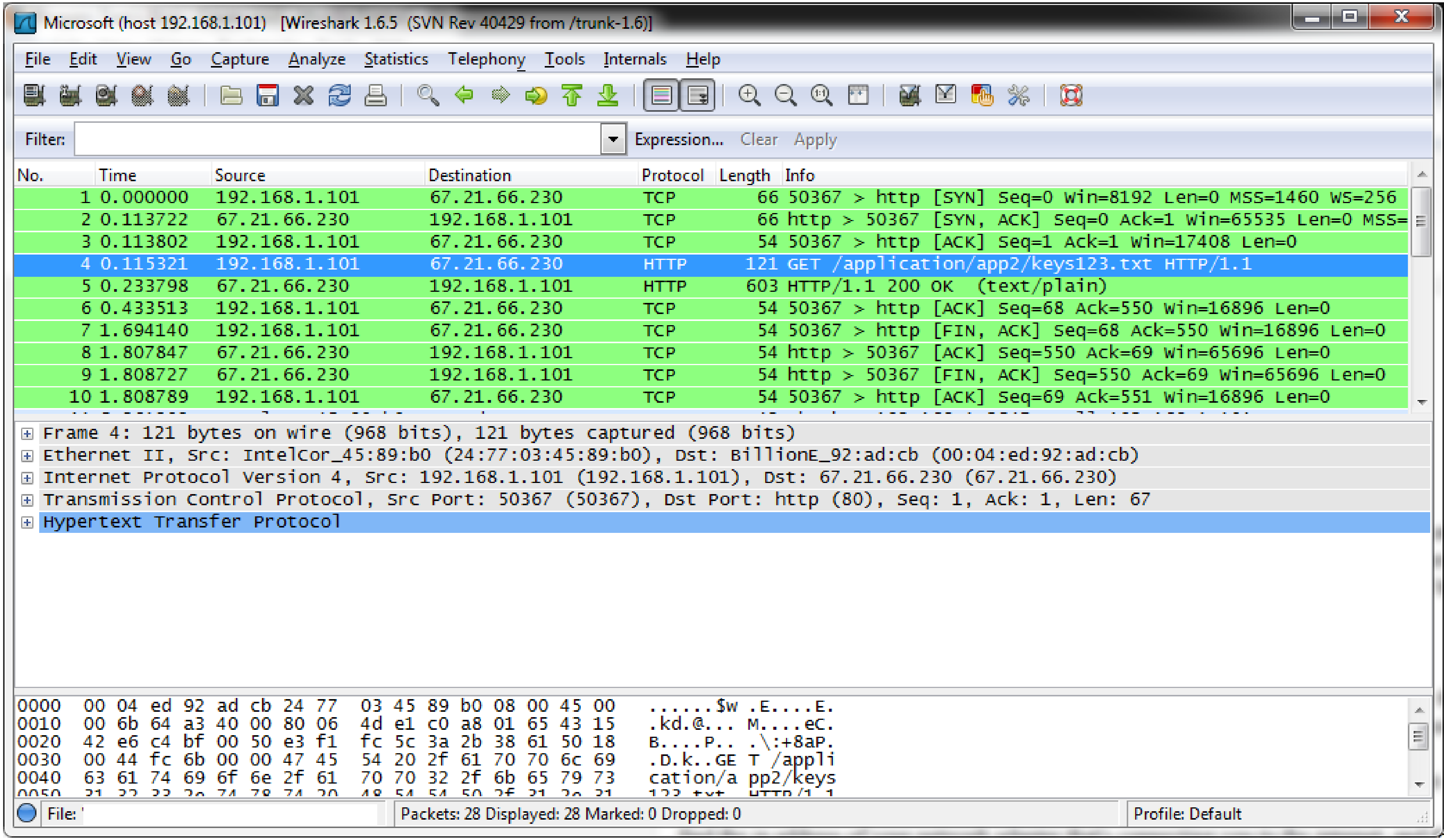
尋找目標：status: send

□ 全字拼寫須符合(W)
□ 區別大小寫(C)
☑ 循環(D)
☑ 透明度

Normal text file   length : 1470915   lines : 3420   Ln : 3397   Col : 1900   Sel : 12 | 0   Macintosh   ANSI   INS

HTS Application 2

- Or use Wireshark


Microsoft (host 192.168.1.101) [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.101   67.21.66.230    TCP          66 50367 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
   2 0.113722  67.21.66.230    192.168.1.101   TCP          66 http > 50367 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
   3 0.113802  192.168.1.101   67.21.66.230    TCP          54 50367 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
   4 0.115321  192.168.1.101   67.21.66.230    HTTP        121 GET /application/app2/keys123.txt HTTP/1.1
   5 0.233798  67.21.66.230    192.168.1.101   HTTP        603 HTTP/1.1 200 OK  (text/plain)
   6 0.433513  192.168.1.101   67.21.66.230    TCP          54 50367 > http [ACK] Seq=68 Ack=550 Win=16896 Len=0
   7 1.694140  192.168.1.101   67.21.66.230    TCP          54 50367 > http [FIN, ACK] Seq=68 Ack=550 Win=16896 Len=0
   8 1.807847  67.21.66.230    192.168.1.101   TCP          54 http > 50367 [ACK] Seq=550 Ack=69 Win=65696 Len=0
   9 1.808727  67.21.66.230    192.168.1.101   TCP          54 http > 50367 [FIN, ACK] Seq=550 Ack=69 Win=65696 Len=0
  10 1.808789  192.168.1.101   67.21.66.230    TCP          54 50367 > http [ACK] Seq=69 Ack=551 Win=16896 Len=0
```

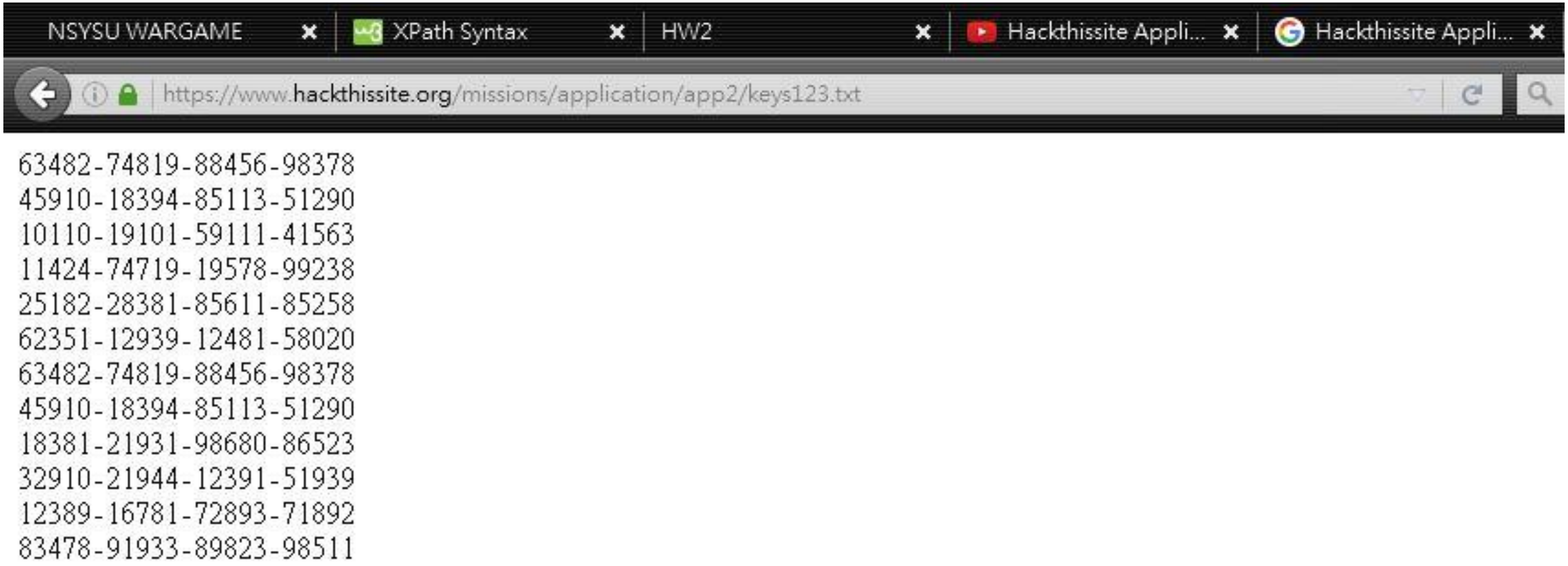
```
⊞ Frame 4: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
⊞ Ethernet II, Src: IntelCor_45:89:b0 (24:77:03:45:89:b0), Dst: BillionE_92:ad:cb (00:04:ed:92:ad:cb)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 67.21.66.230 (67.21.66.230)
⊞ Transmission Control Protocol, Src Port: 50367 (50367), Dst Port: http (80), Seq: 1, Ack: 1, Len: 67
⊞ Hypertext Transfer Protocol
```

```
0000  00 04 ed 92 ad cb 24 77  03 45 89 b0 08 00 45 00   ......$w .E....E.
0010  00 6b 64 a3 40 00 80 06  4d e1 c0 a8 01 65 43 15   .kd.@... M....eC.
0020  42 e6 c4 bf 00 50 e3 f1  fc 5c 3a 2b 38 61 50 18   B....P.. .\:+8aP.
0030  00 44 fc 6b 00 00 47 45  54 20 2f 61 70 70 6c 69   .D.k..GE T /appli
0040  63 61 74 69 6f 6e 2f 61  70 70 32 2f 6b 65 79 73   cation/a pp2/keys
0050  31 32 33 2e 74 78 74 20  48 54 54 50 2f 31 2e 31   123.txt  HTTP/1.1
```

File: ' | Packets: 28 Displayed: 28 Marked: 0 Dropped: 0 | Profile: Default

HTS Application 2

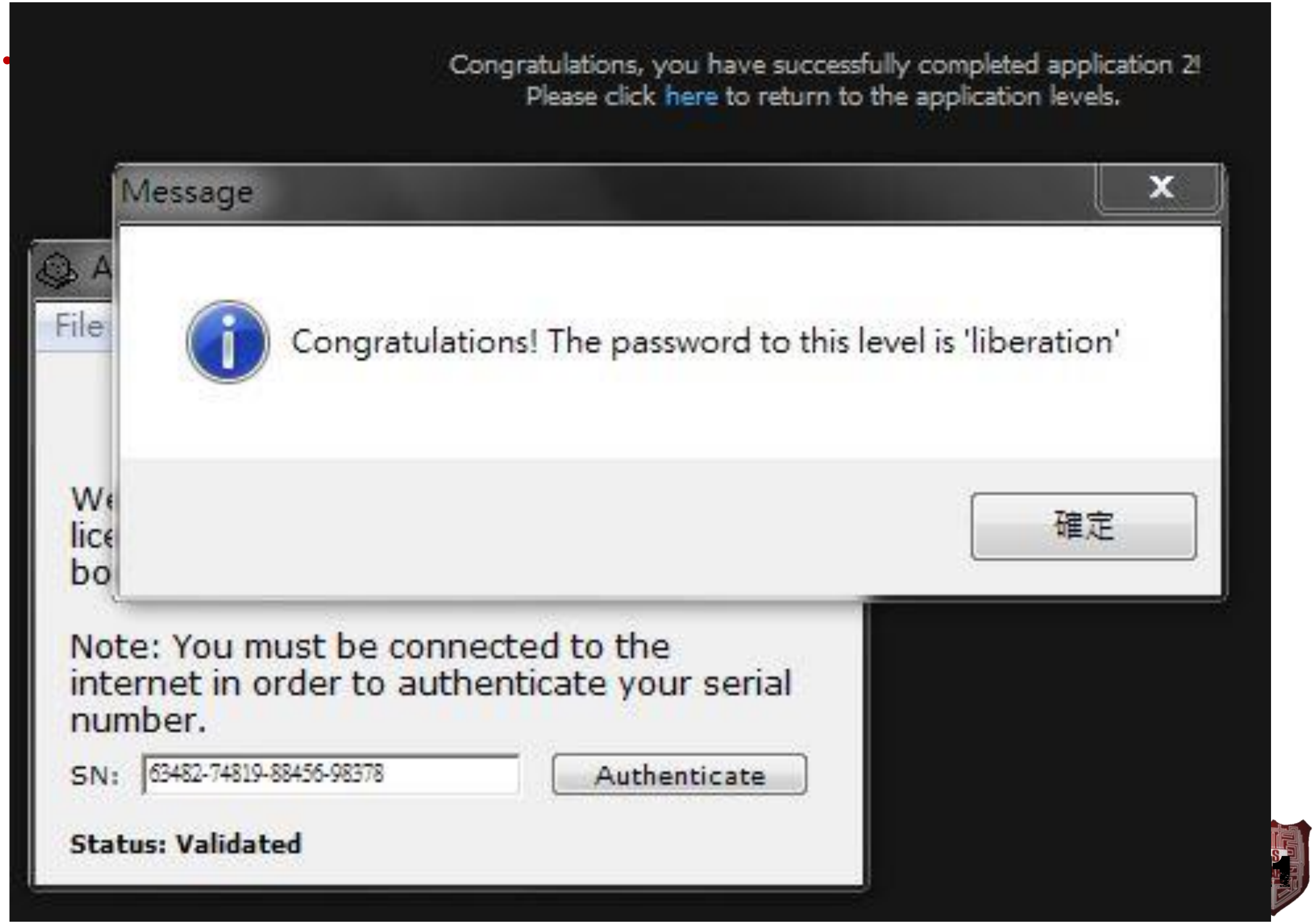
- Connect to Url.



https://www.hackthissite.org/missions/application/app2/keys123.txt

```
63482-74819-88456-98378
45910-18394-85113-51290
10110-19101-59111-41563
11424-74719-19578-99238
25182-28381-85611-85258
62351-12939-12481-58020
63482-74819-88456-98378
45910-18394-85113-51290
18381-21931-98680-86523
32910-21944-12391-51939
12389-16781-72893-71892
83478-91933-89823-98511
```

HTS Application 2



Congratulations, you have successfully completed application 2!
Please click here to return to the application levels.

Congratulations! The password to this level is 'liberation'

We
lice
bo

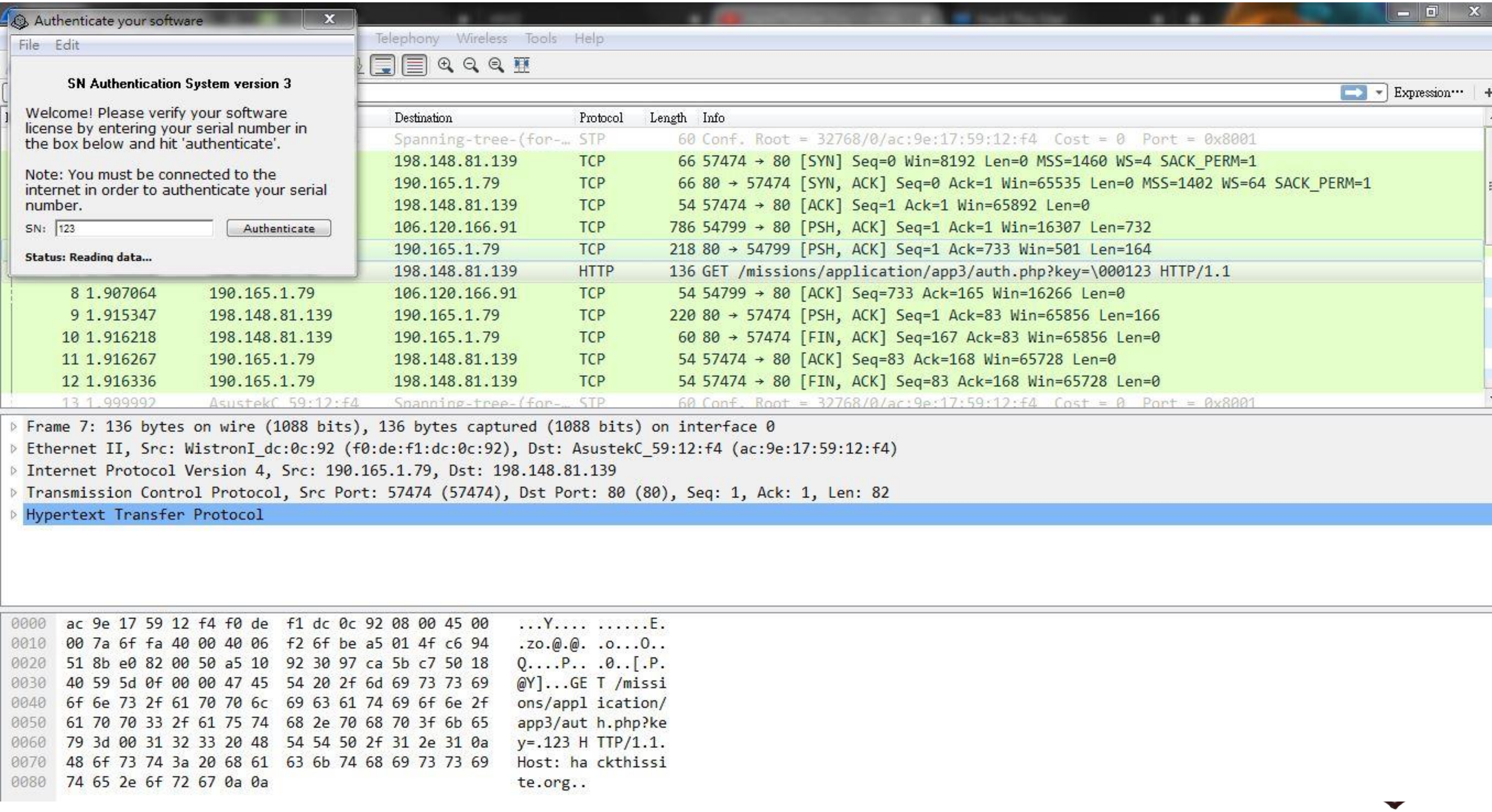
Note: You must be connected to the internet in order to authenticate your serial number.

SN: 63482-74819-88456-98378

Status: Validated

HTS Application 3

- It will stuck at reading data.   It is a bug for App3.



Authenticate your software

SN Authentication System version 3

Welcome! Please verify your software license by entering your serial number in the box below and hit 'authenticate'.

Note: You must be connected to the internet in order to authenticate your serial number.

SN: 123 Authenticate

Status: Reading data...

```
                                   Destination           Protocol  Length  Info
                                   Spanning-tree-(for-…  STP          60 Conf. Root = 32768/0/ac:9e:17:59:12:f4  Cost = 0  Port = 0x8001
                                   198.148.81.139        TCP          66 57474 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
                                   190.165.1.79          TCP          66 80 → 57474 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1402 WS=64 SACK_PERM=1
                                   198.148.81.139        TCP          54 57474 → 80 [ACK] Seq=1 Ack=1 Win=65892 Len=0
                                   106.120.166.91        TCP         786 54799 → 80 [PSH, ACK] Seq=1 Ack=1 Win=16307 Len=732
                                   190.165.1.79          TCP         218 80 → 54799 [PSH, ACK] Seq=1 Ack=733 Win=501 Len=164
                                   198.148.81.139        HTTP        136 GET /missions/application/app3/auth.php?key=\000123 HTTP/1.1
   8 1.907064   190.165.1.79       106.120.166.91        TCP          54 54799 → 80 [ACK] Seq=733 Ack=165 Win=16266 Len=0
   9 1.915347   198.148.81.139     190.165.1.79          TCP         220 80 → 57474 [PSH, ACK] Seq=1 Ack=83 Win=65856 Len=166
  10 1.916218   198.148.81.139     190.165.1.79          TCP          60 80 → 57474 [FIN, ACK] Seq=167 Ack=83 Win=65856 Len=0
  11 1.916267   190.165.1.79       198.148.81.139        TCP          54 57474 → 80 [ACK] Seq=83 Ack=168 Win=65728 Len=0
  12 1.916336   190.165.1.79       198.148.81.139        TCP          54 57474 → 80 [FIN, ACK] Seq=83 Ack=168 Win=65728 Len=0
  13 1.999992   AsustekC_59:12:f4  Spanning-tree-(for-…  STP          60 Conf. Root = 32768/0/ac:9e:17:59:12:f4  Cost = 0  Port = 0x8001
```

```
▷ Frame 7: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
▷ Ethernet II, Src: WistronI_dc:0c:92 (f0:de:f1:dc:0c:92), Dst: AsustekC_59:12:f4 (ac:9e:17:59:12:f4)
▷ Internet Protocol Version 4, Src: 190.165.1.79, Dst: 198.148.81.139
▷ Transmission Control Protocol, Src Port: 57474 (57474), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 82
▷ Hypertext Transfer Protocol
```

```
0000  ac 9e 17 59 12 f4 f0 de  f1 dc 0c 92 08 00 45 00   ...Y.... ......E.
0010  00 7a 6f fa 40 00 40 06  f2 6f be a5 01 4f c6 94   .zo.@.@. .o...O..
0020  51 8b e0 82 00 50 a5 10  92 30 97 ca 5b c7 50 18   Q....P.. .0..[.P.
0030  40 59 5d 0f 00 00 47 45  54 20 2f 6d 69 73 73 69   @Y]...GE T /missi
0040  6f 6e 73 2f 61 70 70 6c  69 63 61 74 69 6f 6e 2f   ons/appl ication/
0050  61 70 70 33 2f 61 75 74  68 2e 70 68 70 3f 6b 65   app3/aut h.php?ke
0060  79 3d 00 31 32 33 20 48  54 54 50 2f 31 2e 31 0a   y=.123 H TTP/1.1.
0070  48 6f 73 74 3a 20 68 61  63 6b 74 68 69 73 73 69   Host: ha ckthissi
0080  74 65 2e 6f 72 67 0a 0a                            te.org..
```